Is Europe Ready for a Pan-European Identity Management System?

Sergio Sánchez García, Ana Gómez Oliva, and Emilia Pérez-Belleboni

When an electronic identity management (eIDM) system users seek to communicate with governments using a different eIDM system, both systems should be linked and should understand each other. To achieve this, the European Union is working on an interoperability framework.

For approximately 10 years, European member nations and economic-area nations have been implementing electronic identity management (eIDM) systems based on their national requirements. Owing to the diversity of eIDM systems, when users of one government's system seek to communicate with governments using a different system, generally both systems should be linked and should understand each other. That is, a user's identity in one system should be understood and accepted by other systems.

For example, imagine that a Spanish citizen holding a Spanish identity card moves to Germany to take a job. He rents out his flat in Spain. While he's working in Germany, his company secures him a contract to work in France for six months. At the end of the year, this citizen must pay taxes in Germany, France, and Spain, and he should be able to do so with a single identity card.

However, technical, social, and legal problems arise from the use of these systems and their interoperability. For that Spanish citizen, technical problems would occur regarding the digital identifier to use because these three countries' certification policies are incompatible. Moreover, there's no common European law on the type of personal data a digital identity should include. Societal acceptance of an identification system is far from equal in all EU member nations, and the legislation and standards aren't uniform. This prompts significant doubts among citizens as to such a system's convenience. This is especially relevant when considering privacy and data protection, where citizens might feel a loss of control over their privacy.

The interoperability of eIDM systems at a pan-European level is a burning issue that has led to several research projects.[1,2] Basically, these projects have culminated in the proposal for a security infrastructure based on a federated model, as we describe in this article.

Criteria for Pan-European eIDM Systems

To successfully establish the interoperability framework, the EU has drawn up a road map with a series of design principles based on the fundamental principle of *subsidiarity*.[3] That is, each member nation must maintain its autonomy and responsibility to continue its eIDM initiatives. These principles give rise to four criteria for a pan-European eIDM system:

- It must be federated; that is, mutual trust must exist between the different governments regarding the identification and authentication methods.
- It must allow member nations to provide multiple

levels of security. The requirements for each member nation's authentication of eIDM systems must be adaptable to its security needs.
- To guarantee the quality of information, each member nation must have one reliable source for each piece of information corresponding to a registered entity, to avoid data duplication and ensure a single correct, official source.
- In member nations in which private companies are trusted, the eIDM system should allow the private sector (for example, financial institutions) to provide eIDM.

In accordance with the Modinis IDM consortium's study,[1] we define *federated identity* as the common approaches for achieving interoperability between eIDM systems that operate in separate (although often similar) contexts.[4] Generally, this can mean one of two things: either a person's user information stored across multiple eIDM systems is virtually reunited, or a user can authenticate across multiple IT systems or even organizations.

We can therefore deduce that federated identity refers to a shared effort to achieve the interoperability of eIDM systems from different environments. In this way, information on a user's identity, possibly spread across different regions, can be gathered so that the user can be identified in one environment and consequently have access to others. The various service providers (SPs) can also access the user's information in the different environments.

A Federated eIDM System

Generally, three entities or agents participate in a federated identity scenario:

- *The user* seeks to access a provider's services. This user's identity is federated. We assume that some form of credential is recognizable by the identity provider (IdP) and possibly the SP.
- *The SP* offers a service to the user after authentication. If the SP recognizes the user's original credentials, it can perform direct authentication. If not, it delegates authentication to the IdP.
- *The IdP* validates the user's credentials and delivers session credentials (such as a Security Assertion Markup Language [SAML] assertion, an X.509 certificate of a very short duration, and the signature of a piece of information) that the SP can validate when authenticating the user before providing a service.

Taking into account the participating entities and exchanges (see Figure 1), we could say that a federated eIDM system is a sequence of entities that transforms a user credential (that, in theory, SPs don't need to understand) into a session credential. This session credential is something that SPs can fully understand and will serve as the basis for deciding whether to provide the requested service.

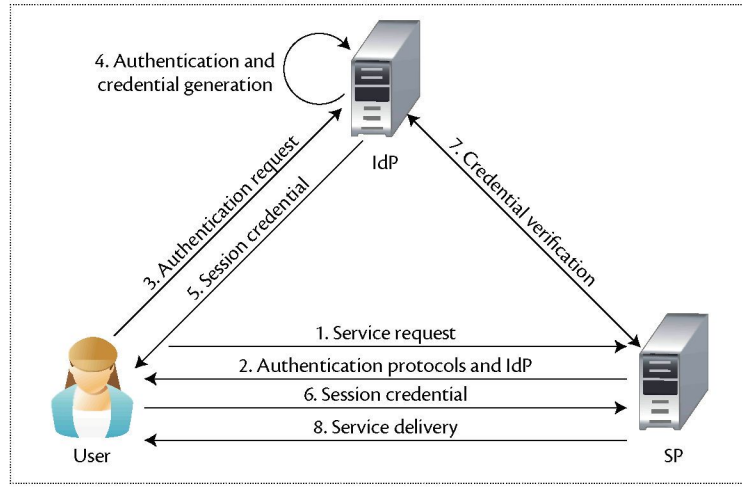

Figure 1. Interactions in an abstract federated electronic identity management (eIDM) system model. Although this example shows a federated eIDM system in which the service provider (SP) initiates federation, in some systems, the identity provider (IdP) initiates federation.

Federated identity extends the eID's use as an internal aspect of one SP into something common to multiple SPs. This change can evoke complicated management processes related to how the identity is registered, revoked, and modified in an IdP. This exposes federated identities to new security risks that must be counteracted.[5]

In an e-government eIDM system, the use of federated identity usually means that two administrations decide to mutually trust each other's identification and authentication methods. So, although federated identity depends on establishing trust and involves greater security risks, it constitutes a key factor in achieving interoperability between the different countries' eIDM systems.

Current Pan-European eIDM Systems

Since the publication of the EU's e-government action plan in 2006[6] and as a result of subsequent directives for all member nations, several initiatives now focus on pan-European interoperability among eIDM systems. Here, we look at the most significant proposals for such systems. These proposals have influenced development toward the present pan-European model, whose viability is being tested in the Stork project.

The Modinis IDM Study

One of the first projects dedicated to eIDM system interoperability was the Modinis IDM study.[1] It

defined key enablers that all European nations should adopt to provide

- rapid e-government services in a mobile, ubiquitous environment,
- authentic data repositories (capable of guaranteeing that information is accurate and authentic for a certain entity), and
- compatible methods and authentication levels.

The study defined an infrastructure based on a federated model that relies on (at least one) IdP in each member nation to authenticate an entity at a national level and decide the level of trust to grant to different authentication processes in each nation. In this model, the authentication requirements for a specific service in a nation would honor the authentication levels and mechanisms used in another nation as equivalents on the basis of a set of previously defined criteria. This would make an EU-specific infrastructure unnecessary.

TLS-Federation

The TLS-Federation[2] (where TLS stands for Transport Layer Security) model uses the public-key infrastructure (PKI) during authentication. It employs a user-centered approach; users directly manage identity and privacy attributes.

TLS-Federation is a proposal for system federation based on sufficiently known and tested standards—specifically, the TLS protocol and X.509 certificates. So, TLS-Federation applies the TLS protocol in its client authentication mode based on an X.509 certificate to a federated identity environment. The fundamental idea is that IdPs will deliver X.509 certificates as security assertions to SPs via the TLS handshake protocol. The X.509 assertions act as session credentials with a limited life span and take the place of any other type of security token, such as SAML assertions.

If we compare TLS-Federation with other proposed eIDM systems, the solution proves viable, particularly in creating a cost-efficient infrastructure. It's the only solution that requires few (if any) additional installations and doesn't require converting session credentials for a member nation's domain to access the pan-European domain.

Nevertheless, TLS-Federation has its drawbacks. For example, it can work only with X.509 certificate eIDs, and not all countries are ready to implement these. It would require a detailed study of the possible use of TLS extensions that can map non-X.509 certificate user credentials into X.509 session certificates. However, although the exclusive management of credentials based on X.509 certificates is a current challenge, it shouldn't be in the long run because the trend in EU member nations is toward using such credentials to robustly identify citizens and entities.

If EU member nations implement a strong authentication system and employ government IdPs based on PKI, then TLS-Federation might be an option for pan-European authentication. However, this solution doesn't enable eIDM system integration for countries whose current systems aren't based on certificates. So, although it's a good solution, it isn't presently applicable in the EU.

Regardless, studying the authentication-related features in TLS-Federation is worthwhile because they require little integration work. Every part of the technology is available and is supported by most operating systems, search engines, and webservers—it's simply a matter of activating the system.

Guide

The Guide project (http://istrg.som.surrey.ac.uk/projects/guide/overview.html) proposed a model for European ID interoperability based on the concept of a federated eIDM system network in which members, users, administrators, and enterprises can exchange identity information without compromising their privacy and security. This model requires the prior affiliation of members in circles of trust—that is, federations of SPs and IdPs that have established formal relations and operational agreements and whose service consumers can carry out transactions.

There are now both technical solutions that enable this type of federation and examples of good practices. InCommon (www.incommon.org) is a common-trust framework that includes trustworthy shared management of access to online resources in support of education and research in the US. EduGain (www.edugain.org) enables global collaboration in research by linking 30 European academic networks and organizations to each other, as well as to other regions of the world.

In the EU, a number of these federations and circles of trust have been established for different administrative and commercial stakeholders. Particularly, many member nations are involved in developing such federations at a national level. However, many of these federations have been or are being established in isolation from one another. This doesn't comply with Guide principles, which call for a pan-European federation of identities.

Stork

Incorporating ideas from the Guide project, the Stork project (*S*ecure Iden*t*ity acr*o*ss Bo*r*ders Lin*k*ed; www.eid-stork.eu) proposed a pan-European eIDM system. This project (ended in December 2011 but currently extended as Stork 2.0) developed and tested common specifications for mutual, secure national eIDs of participating countries. The EU is adopting its results as a

model for guidelines for member nations to follow to achieve a pan-European eIDM system.

Stork's proposed model is based on preliminary studies by IDABC (Interoperable Delivery of European eGovernment Services to Public Administrations, Business, and Citizens)[7] that describe a federated model for interoperability that's technologically neutral and supports multiple levels of authentication. It relies on a proxy and requires creating national IdPs (at least one per country). Stork combines this system of IdPs with a network of gateways or proxy SPs called PEPS (pan-European proxy services). Figure 2 illustrates the model.

PEPS would be created at a national level (although the model allows for one at a centralized EU level or even a mixed model) in which some countries would rely on national PEPS, whereas others would use European PEPS. PEPS would be useful mainly in overcoming technical problems that arise when a broad range of identification and authorization solutions exists for access to services, as is the case in the EU. For example, one citizen might want to use a login to access a service, whereas another wishes to use an eID card. Assuming that the application's owner accepts both identification methods, the technical infrastructure must be able to support both solutions. So, the Stork model defines four quality authentication assurance (QAA) levels.[8] The lowest level would correspond to eID solutions based on users and passwords; the highest level would occur through an X.509 certificate with an eID or smart card.

The four QAA levels takes into account each solution's organizational and technical components. On the basis of these levels, national identity solutions can be mapped onto previously defined and agreed-upon patterns. This will allow the Stork model to be applied in all countries, regardless of which identification systems they allow. So, if different QAA levels are allowed access to a service, the technical infrastructure should be able to support them.

This is where PEPS come into play. They mainly connect SPs with the proper IdPs in each country, redirecting authentication requests to the pertinent IdP, and validate the trust and security of the identity information that the IdPs sent. So, all the PEPS form a circle of trust in accordance with the solutions specified by the Liberty Alliance (www.projectliberty.org). Regarding technologies, Stork suggests using SAML assertions to transport identity attributes from IdPs to SPs via PEPS. The project seeks to rely on, as far as possible, open standards. It provides a solution to interoperability at a pan-European level that doesn't require modifications to national eIDM systems, thus taking into account the use of all identification and authorization models deployed in EU member countries.

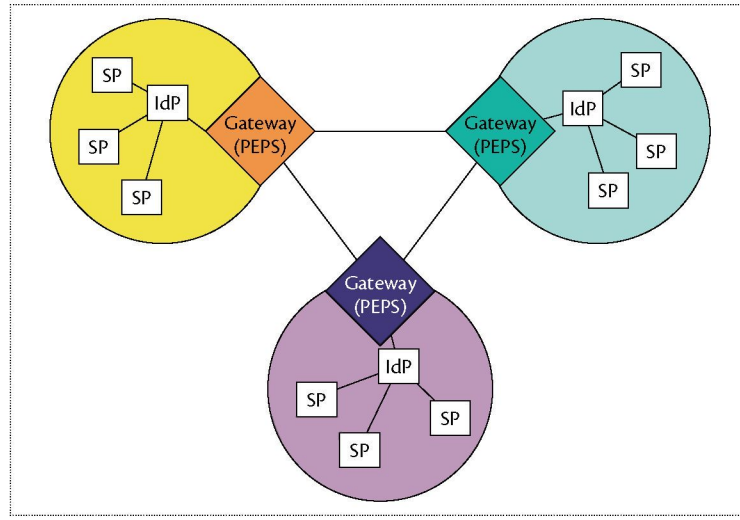

Figure 2. Stork's proposed model. Stork combines a system of IdPs with a network of gateways or proxy SPs called PEPS (pan-European proxy services).

Remaining Challenges

Because the EU's adopted solution implements a federated infrastructure, it can separate service provision from the digital-identity-related processes necessary to provide the service (namely, user registration, generation and storage of identification data, and authentication). Because the system is multilevel, it can (theoretically, with no major changes) incorporate all countries with their own eIDs and eIDM systems, thus accelerating the implementation of a pan-European eIDM system. However, there are still barriers to overcome if this solution is to be feasible.

Creating a Federated System

An analysis of the state of affairs regarding the legislation and implementation of eIDM systems in Europe shows distinctions across member nations. Some have clearly implemented eIDs and eIDM systems, whereas others are only beginning the process. A single, global focus on eIDM system implementation is therefore inadequate because not all countries are beginning from the same point, and every country handles data and deals with citizens differently.

Fortunately, the EU's solution requires no deployment or minimal deployment of an EU-level infrastructure. Also, countries that are less technologically advanced or that have fewer resources can easily and quickly be incorporated in the European federated system. Reaching total integration will require the ability to incorporate less advanced countries in a way that's simple and not onerous—economically or technologically—by means of central PEPS.

A federated system should be able to create a circle of

trust among the infrastructures of all member countries and enable the easy inclusion of future countries. Such a system will allow creation of a pan-European infrastructure with hardly any changes to current systems. Toward that end, possible solutions could use identity portals in each country to handle internal authentication and to manage trust placed in other countries' eIDM systems. Or, they could rely on service access proxies in each country. These solutions would adapt perfectly to federation and the idea of maintaining the systems already implemented in the member nations as much as possible.

Providing Transparency

Because of existing systems' heterogeneity and different countries' authentication and authorization mechanisms, a pan-European system must be able to map identity tokens delivered by the one country's eIDM system to their counterparts in another country. This will help make access to services as transparent as possible to users.

Avoiding Redundancy

The interoperability solution proposed by Stork still faces many stumbling blocks. The first involves managing information, specifically concerning the reliability and quality of the data handled. Typically, existing eIDM systems have no single data source, which could give rise to duplication problems and lack of coherence. As we mentioned earlier, every country must have a single reliable source for every piece of information pertaining to a registered entity, thus preventing duplication and guaranteeing accurate and official data. This is a concern because many European countries have several administration levels (local, regional, and national) that often rely on data that isn't synchronized, thus leading to redundancies and inconsistencies.

Integrating the Private Sector

Except for Stork 2.0, none of the projects we discussed considered employing the private sector to provide the eIDM system infrastructure or to be SPs. This is the case even though the EU road map specifies that the development of private-sector applications that rely on public eIDM system infrastructures should receive special attention.[3]

The technical challenges of integrating the private sector often involve the discouraging task of integrating proprietary and nonstandard systems with federated authorization systems. Moreover, the social challenges seem insurmountable, as evidenced by the insufficient integration between private entities and governments in the same country. Presumably, a certain degree of trust in these environments should exist because data custody and information protection are regulated and legislated under the same criteria. Nevertheless, if full interoperability hasn't been achieved in a bounded environment such as public administration, it seems highly unlikely that cross-border identification and authentication solutions such as those proposed in this article will be adopted in the short term for service provision in the private sector.

Even more questions arise when the private sector refers to small- and medium-sized private enterprises, which have fewer resources and less specialized personnel. Present proposals barely address possibilities for integration with industry and offer solutions solely for interoperability in the public sector. How can such solutions integrate with the identity environments most commonly used in industry? From our perspective, this issue has received little attention, and little identification integration exists between the public and private sectors. In any given country, few service provision environments use that country's available public eIDM systems. (A remarkable and isolated example of using public X.509 certificates in the private sector comes from some electronic bank services, which accept these certificates to verify users' identities.)

The Stork 2.0 project aims to tackle these problems and generate solutions that are viable in the EU. Its goal is to achieve the convergence of the private and public sectors in an operational framework and infrastructure encompassing eID for secure electronic authentication of citizens.

Accommodating Electronic Signatures

Another problem is the interoperability of electronic signatures. European legislation lets anyone use his or her eID to sign any piece of information going to a recipient, who could be in a different EU country. This means that the entity receiving a signed document must be able to verify the signature, irrespective of the signing entity's eID.

Although the technical validation of signatures has its challenges regarding scaling, the real problem for the receiving party is the risk implied by accepting the signature. This risk is determined by the legal situation, the cryptography's quality, the liability situation, and the certification authority's trustworthiness. To solve these problems, initiatives are developing guidelines, specifications, and pilot solutions to overcome the lack of interoperability between national schemes for electronically signed tender documents. It's to be hoped that these problems will disappear and that signature verification can be carried out in the future with full guarantees.

European countries have made significant efforts to achieve interoperability among the different national eIDM systems. Although we believe that

pan-European eIDM systems are technologically viable, we recognize that interoperability in identity management isn't just a technological problem. Significant legal barriers affect cross-border and cross-sector relations, and the EU should provide the appropriate legal support before achieving the desired interoperability.

Regarding the possible alignment of present solutions with future technology trends, these solutions' viability depends on the path that public administrations take regarding service provision. Present trends appear to point toward providing services in the cloud. In the medium term, this will probably involve each government creating its own isolated cloud. Here, the Stork project might become viable with minimal modifications. As we've seen, present eIDM systems and service provision environments constitute independent islands managed by a certain public administration or country. Stork proposes an interoperability solution for these islands. At first glance, the fact that the islands become clouds wouldn't appear to pose greater problems for this solution, which would interconnect and ensure interoperability between clouds through proxies.

We believe the EU is moving in the right direction. Single virtual-identity domains, such as the one in Stork, could be useful for global environments or services requiring authentication mechanisms that enable smart, automatic user registration and ensure smooth identity transition across SPs.

Global online identification will pose new challenges and solutions. A pan-European interoperability infrastructure will be a first step toward more complex identity systems that allow secure management of new user-identification attributes. Further research must proceed in the semantic interoperability of attributes, with the aim of achieving comprehension across different eIDM systems. To the extent that these objectives are met, citizens will be able to use online services with greater assurances of security than are currently available and, therefore, with more satisfaction. ■

Acknowledgments

This article is part of research we're conducting in the Talisec+ project (a framework for knowledge-based management of accessible security guarantees for personal autonomy; TIN2010-20510-C04-01), supported by the Ministry of Education and Science of Spain through the National Plan for R+D+I (research, development, and innovation).

References

1. *Modinis Study on Identity Management in eGovernment*, tech. report, European Commission, 2006; http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_conceptual_framework.pdf.
2. P. Bruegger, D. Hühnlein, and J. Schwenk, "TLS-Federation—a Secure and Relying-Party-Friendly Approach for Federated Identity Management," *Proc. Special Interest Group on Biometrics and Electronic Signatures* (BIOSIG 08), Gesellschaft für Informatik, 2008, pp. 93–106.
3. *A Roadmap for a Pan-European eIDM Framework by 2010*, ver. 1.0, European Commission Information Soc. and Media Directorate-General, 2007; http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf.
4. "Federated Identity," Modinis-IDM consortium, 2005; https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/FederatedIdentity.
5. C. Steel, R. Nagappan, and R. Lai, *Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management*, Prentice Hall, 2005.
6. *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*, Commission of the European Communities, 2006; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0173:FIN:EN:PDF.
7. J. Majava and H. Graux, *eID Interoperability for PEGS: Common Specifications for eID Interoperability in the eGovernment Context*, tech. report, European Communities, 2007; http://ec.europa.eu/idabc/servlets/Doc467b.pdf?id=30989.
8. B. Hulsebosch, G. Lenzini, and H. Eertink, *Quality Authenticator Scheme D2.3*, ICT Policy Support Programme, 2009.